Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A system, comprising:

a control center to coordinate thwarting attacks on a ~~victim~~ data center that is coupled to a network, the control center including:

a communication device, coupled to a physically separate network from the network that the data center is coupled, to receive data from a plurality of monitors[[,]] dispersed through the network that the data center is coupled to, with the monitors sending data collected from the network that the data center is coupled to over ~~a redundant network, with~~ the ~~redundant network being a~~ physically separate network from the network that the plurality of monitors collect data from;

a computer system, the computer system comprising:

a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic; and

an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center.

Claim 2 is canceled.

3. (Original) The system of claim 1 wherein the data analyzed by the control center is sampled packet traffic and/or accumulated and collected statistical information about network flows.

4. (Original) The system of claim 1 wherein the control center aggregates traffic information and coordinates measures to locate and block the sources of an attack.

5. (Currently Amended) The system of claim 1 wherein the physically separate is a telephone ~~control center is a hardened site and the redundant network is a private redundant~~ network.

6. (Previously Presented) The system of claim 1 wherein monitors include gateways that are disposed at the victim data center and data collectors that are disposed in the network, and the analysis process executed on the control center analyzes data from gateways and data collectors dispersed throughout the network.

7. (Original) The system of claim 1 wherein the analysis process classifies attacks and determines a response based on the class of attack.

8. (Original) The system of claim 7 wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing.

9. (Currently Amended) A method, executed on a computer system, the method comprises:

receiving by the computer system data from a plurality of monitors, dispersed through the network, with the monitors sending data collected from the network over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from;

analyzing in the computer system the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic; and

determining in the computer system a filtering process to install to eliminate the malicious traffic from entering the victim data center.

Claim 10 is canceled.

11. (Currently Amended) The method of claim 9 further comprising:

aggregating in the computer system traffic information and coordinating measures to locate and block the sources of an attack.

12. (Currently Amended) The method of claim 9 wherein receiving and analyzing are performed by the computer system that is a control center coupled to the monitors via the hardened, redundant network.

13. (Original) The method of claim 9 wherein plurality of monitoring devices are data collectors dispersed throughout the network and at least one gateway device that is disposed adjacent the victim site to protect the victim and wherein analyzing comprises:

analyzing in the computer system ~~at a control center~~ data from the at least one gateway and the data collectors dispersed throughout the network.

14. (Original) The method of claim 9 wherein analyzing comprises:

classifying attacks and determining a response based on the class of attack.

15. (Original) The method of claim 14 wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing.

16. (Currently Amended) The method of claim 14 further comprising:

sending requests to gateways and/or data collectors ~~for~~ to send data pertaining to an attack to the control center.

17. (Previously Presented) The method of claim 14 further comprising:

sending requests from the control center to gateways and/or data collectors for requests to install filters to filter out attacking traffic.

18. (Currently Amended) A computer program product to coordinate thwarting attacks on a victim data center that is coupled to a network comprises instructions to cause a computer to:

receive data from a plurality of monitors, dispersed through a first network that is coupled to the victim data center, with the monitors sending data collected by the monitors from the first network over a redundant, network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from;

analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic;

determine a filtering process to eliminate the malicious traffic from entering the victim data center[[;]] and

~~aggregate traffic information and coordinating~~ coordinate measures to locate and block the sources of an attack.

19. (Original) The computer program product of claim 18 wherein instructions to receive and analyze are performed by a control center coupled to data collectors via a hardened, redundant network.

Claim 20 is canceled.

21. (Currently Amended) A system, comprising:

a computer system, configured as a control center to coordinate thwarting of a denial of service attack on a victim data center that is coupled to a network, the control center, executing: ~~including~~:

a communication process that executes on the computer system ~~and device~~ to receive statistical data from and send messages to a plurality of monitors dispersed through the network,

with the communication device and process sending the messages and receiving the statistical data from the monitors over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from; and

~~a computer system, the computer system comprising:~~

an analysis process that executes on the computer system to analyze the statistical data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic and to send the messages to the monitors to control monitors in the network to coordinate thwarting an attack on the victim data center; and

an aggregate process to aggregate traffic statistics from the plurality of monitors to use in coordinating measures to locate and block the sources of an attack.

22. (Currently Amended) The system of claim 21 further comprising:

a process that executes on the computer system to select a filtering process to eliminate the malicious traffic from entering the victim data center.

Claim 23 is canceled.

24. (Currently Amended) The system of claim 21 further comprising:

a process that executes on the computer system to classify attacks and determine a response based on the class of attack.

25. (Previously Presented) The system of claim 21 wherein the classes of attack are denoted as a low-grade attack with spoofing, a low-grade attack without spoofing and a high-grade attack whether spoofing or non-spoofing.

26. (Previously Presented) The method of claim 14 further comprising:

sending requests to gateways and/or data collectors to send data back to the system pertaining to an attack.

27. (Previously Presented) The system of claim 21 further comprising:

a process to send requests from the control center to gateways and/or data collectors to install filters to filter out attacking traffic.